[in]security

by Gary McGraw

Is Your Mac Really More Secure?

Apple Macintosh users are quick to point out the dearth of malware, viruses, and security problems in the OS X world. Compared to the Windows/Intel Win32 platform, Mac OS X looks like an attractive alternative, at least when malware is the deciding factor. Win32 machines have suffered from any number of spectacularly successful malcode attacks over the years, and the problem shows no signs of abating.

To be completely fair, there have been a few minor OS X-related viruses, and Apple regularly releases security patches. But Win32 is in much worse shape, and Mac users gloat about this all the time.

Mac users are in for a big surprise. The very pride they take in the security of their beloved boxes is a powerful attracter for curious and sometimes malicious hackers. Combine that with cross-platform malware that leverages the widespread outbreak potential of a Win32 exploit, and Mac users will find themselves quickly swept up in the malware deluge.

> The very pervasiveness of Win32 presents a clear and present danger to Mac users.

What follows is a simple and perhaps ironic prediction of how prideful Mac users will be taken down a notch.

BITING INTO APPLE

Security-savvy Mac users believe that the Win32 target is so enticing, so big, and so easy to hit that malware writers will pay no attention to their little corner of the universe. They ask why anyone would bother writing an exploit just to round up a few measly Macs.

The answer is that Macs represent a challenge. Hackers set out to solve puzzles, take things apart, understand how things work, and on occasion cause trouble. Building an attack that works on Macs will be a badge of honor proudly worn, and work is already under way to see who gets the prize.

The irony is that the very pervasiveness of Win32 and its ease of compromise present a clear and present danger to Mac users. Macs run PC software. They almost all run Microsoft Office, and they include the ubiquitous Web server and Outlook clients. Most importantly, they're densely interconnected to thousands and thousands of Win32 machines. Rather than being above trouble, they're surrounded by it. A clever attacker can take advantage of this Achilles' heel with cross-platform malware aimed at Win32 and Mac computers.

PRIDE BEFORE THE FALL

Cross-platform attacks are complicated and require explicit knowledge of chips and OSs. However, these barriers are easily overcome by sophisticated attackers. A number of cross-platform payloads designed to run against multiple chips have already been created and circulated in the wild, including one that works for HP 9000 and Intel chips, and another that works for MIPS and Intel. RISC chips have also been explored fairly deeply, so an attacker can combine that knowledge to create a payload that works for Intel and PowerPC G4, the RISC-based chip behind the Mac. Once that happens, the road to cross-platform viruses that conquer the Mac will essentially be complete.

Payloads also already exist that cross traditional OS boundaries. For example, the Simile.D virus, which debuted in 2002, targeted Win32 and Linux platforms. The OS X's embrace of the Berkeley Software Distribution (BSD) kernel can only serve to speed along a cross-platform attack because Linux and BSD, both Unix variants, share many design concepts and are susceptible to the same kinds of attacks.

Though there have been no confirmed sightings of cross-platform payloads targeting Win32 and OS X, it's only a matter of time before they emerge. Propagation of such malware will follow the astounding Win32 release curve, covering the planet in a matter of hours. And the "superior"-—and completely surrounded—Mac users will be in for it this time.

Gary McGraw is CTO of Cigital, a software quality management consultancy. He is co-author of *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and *Java Security* (Wiley, 1996). Reach him at gem@cigital.com.